UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/077,531	02/14/2002	Douglas Michael Cohen	1-1-1-1	3526

7590 02/15/2006

Ryan, Mason & Lewis, LLP
Suite 205
1300 Post Road
Fairfield, CT 06430

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/077,531	COHEN ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on January 5, 2006. Independent claim 11 has been amended. Claims 1-14 are pending.

Response to Arguments

Applicant's arguments filed January 5, 2006 have been fully considered but they are not persuasive.

Applicant argues that Nelson teaches that, "... the process of newly generated key pairs is priodically repeated as designed. Alternatively, the transition to the newly assigned pair may be time-dependent. In that case, a client that fails to switch over to the new key pair would be required to re-authenticate to gain access to the network" (Remarks, Page 6).

Examiner responds that Nelson only adds a limitation to what the instant application is claiming. According to Nelson, "once the new keys have been transmitted to all associated clients transmits with the latest generated transmit key, the access point ***switches over*** to its newly assigned transmit key"; therefore, should this switching over to the newly assigned transmit key take place as it is expected to, no re-authentication is necessary to gain access to the network. In another word, Nelson's disclosure enforces generating at least one new key after a selectable period of time in order to take advantage of key-based sessions, without requiring to re-authenticate the client for gaining access to the network (Par. 0014 and 0023).

Allowable Subject Matter

Upon further consideration, the indicated allowability of claim 9 is withdrawn in view of the newly discovered features of the existing reference(s), namely Nelson et al., (U.S. Publication No. 2003/0095663).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, and 9-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Nelson et al., (U.S. Publication No. 2003/0095663 and Nelson hereinafter).

Regarding claims 1 and 13, Nelson discloses a method to improve security in a wireless network, the method comprising:

determining a time period, the time period indicating when at least one new key is to be generated (Page 3, Par. 0023);

loading a number of keys in a controller (i.e., client transmit key and client receive key), the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still

communicate in a secure manner on the wireless network, and communicating the keys from the controller to the device (Page 3, Par. 0022).

Regarding claim 2, Nelson discloses wherein the time period further indicates when devices communicating with the wireless network are to be re-authenticated (Page 2, Par. 0014).

Regarding claims 3 and 11, Nelson discloses a method to improve security in a wireless network, the method comprising: loading a time period, the time period indicating when at least one new key is to be generated (Page 3, Par. 0023);

loadinlg a plurality of keys, selecting one of the keys as a local transmit key and selecting the other keys as receive keys (i.e., in Fig. 3, each key is marked, one as a client receive key and the other as a client transmit key), performing the following steps every time period: (i) generating at least one new key, (ii) using the at leat one new key to replace, for each of the at least one keys, one key of the plurality of keys, the at least one new key and any keys not replaced comprising a new plurality of keys, and (iii) selecting a key of the new plurality of keys as a local transmit key, the local transmit key for a current time period selected to be different than the local transmit key for an immediately proceeding time period (i.e., exchanging the existing key pair with a newly generated pair, either after a certain number of frames have been processed by the access point or after a selectable period of time)(Page 3, Par. 0021-0023).

Regarding claim 9, Nelson discloses wherein the method further comprises the steps of:

determining, every time period, at least one new key, and replacing one of the keys with at least one new key when the plurality of keys reaches a predetermined number of keys, else adding the at least one new key to the plurality of keys (i.e., in the event a plurality of such keys are already registered, the least recenetly used or oldest pair is over-written)(Page 3, Par. 0023).

Regarding claims 4 and 10, Nelson discloses wherein the method further comprises the step of selecting one of the keys as a local transmit key, and the step of communicating the keys to a device further comprises the step of communicating to the device that a particular key of the keys is to be a transmit key for the device, wherein the particular key is selected to be different from the local transmit key (Page 3, Par. 0022).

Regarding claim 12, Nelson discloses a method to improve security in a wireless network, the method comprising:

a memory that stores computer-readable code, and a processor operatively coupled to the memory, said processor configured to implement the computer-readable code (Pages 2-3, Par. 0019-0020), said computer-readable code configured to:

determining a time period, the time period indicating when at least one new key is to be generated (Page 3, Par. 0023);

loading a number of keys in a controller (i.e., client transmit key and client receive key), the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the wireless network, and communicating the keys from the controller to the device (Page 3, Par. 0022).

Regarding claim 14, Nelson discloses a method performed on a device communicating with a wireless network, the method comprising:

loading a number of keys in the device, the number set so that the device can miss being re-authenticated for a predetermined number of time periods and still communicate on the wireless network, using at least one key of the keys as a tansmit key, and using at least one key of the keys as receive keys (Page 3, Par. 0022-0023).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nelson et al., (U.S. Publication No. 2003/0095663 and Nelson hereinafter), in view of Sowa et al., (U.S. Publication No. 2002/0154781 and Sowa hereinafter).

Teachings of Nelson with regard to limitations of claim 1 have been discussed previously.

Regarding claim 5, Nelson does not expressly disclose wherein the controller is operating in a mixed mode and a number of keys are loaded.

However, Sowa discloses wherein the controller is operating in a mixed mode, the step of loading a plurality of keys comprises the steps of:

loading a fixed key, and loading at least one additional key, wherein the number of keys comprises the fixed key and the at least one additional key (Page 2, Par. 0026-0031); and

the step of selectinlg one of the keys as a local transmit key comprises the step of selecting the fixed key as the local transmit key (i.e., DCK, Derived Cipher Key.The DCK is used for inbound traffic encryption and also for the outbound individually addressed traffic to the MS for the duration of any session)(Pages 3-4, Par. 0041-0053).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Nelson with the teachings of Sowa because it would allow to include selectinlg one of the keys as a local transmit key comprises the step of selecting the fixed key as the local transmit key as disclosed by Sowa. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Sowa to share one piece of information between the users, which permits only those users knowing it to properly decrypt the message (Sowa, Page 1, Par. 0002).

Regarding claim 6, Nelson dislcoses wherein the at least one additional key is one key and the predetermined number of time periods is one (Page 3, Par. 0022-0023).

Regarding claim 7, Nelson discloses a client receive key and a client transmit key (Page 3, Par. 0022).

Nelson does not expressly disclose wherein the controller is operating in a standard mode and communicating the at least the three keys to the device.

However, Sowa discloses wherein: the controller is operating in a standard mode, and the step of loading a number of keys comprises loading at least three keys, the method farther comprises the steps of: selecting one of the keys as a local transmit key, and selecting the other keys as local receive keys (i.e., as keys are passed between devices that require different encryption keys, one device receives a message, decrypts it with one key, and re-encrypts the result with another key for the next device)(Page 2, Par. 0086-0090); and

the step of communicating the keys comprises communicating the at least the three keys to the device (Pages 3-4, Par. 0041-0053).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Nelson with the teachings of Sowa because it would allow to include communicating the at least the three keys to the device as disclosed by Sowa. This modification would have been obvious because one

of ordinary skill in the art would have been motivated by the suggestion of Sowa to to provide secure transfer of key material among the system devices (Sowa, Page 1, Par. 0023).

Regarding claim 8, Nelson discloses wherein the at least three keys are three keys and wherein the predetermine nnmber of the time periods is one (Page 3, Par. 0022-0023).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
Feb.8, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100